

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-189721

(P2001-189721A)

(43) 公開日 平成13年7月10日 (2001.7.10)

(51) Int.Cl. ⁷	識別記号	F I	サーチコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R
H 0 4 L 9/12		H 0 4 L 9/00	6 0 1 E
			6 3 1

審査請求 未請求 請求項の数 8 O L (全 19 頁)

(21) 出願番号 特願2000-363624(P2000-363624)

(22) 出願日 平成12年11月29日 (2000. 11. 29)

(31) 優先権主張番号 1 9 9 5 7 3 8 7. 5

(32) 優先日 平成11年11月29日 (1999. 11. 29)

(33) 優先権主張国 ドイツ (D E)

(31) 優先権主張番号 1 9 9 5 8 0 0 4. 9

(32) 優先日 平成11年12月2日 (1999. 12. 2)

(33) 優先権主張国 ドイツ (D E)

(31) 優先権主張番号 1 0 0 0 2 1 8 3. 2

(32) 優先日 平成12年1月19日 (2000. 1. 19)

(33) 優先権主張国 ドイツ (D E)

(71) 出願人 590000248

コーニンクレッカ フィリップス エレク
トロニクス エヌ ヴィ

Koninklijke Philips
Electronics N. V.

オランダ国 5621 ベーアー アインドー
フェン フルーネヴァウツウェッハ 1

(72) 発明者 クリストフ ヘルマン

ドイツ連邦共和国, 52064 アーヘン, カ
ゼルネンシュトラッセ 6

(74) 代理人 100070150

弁理士 伊東 忠彦 (外1名)

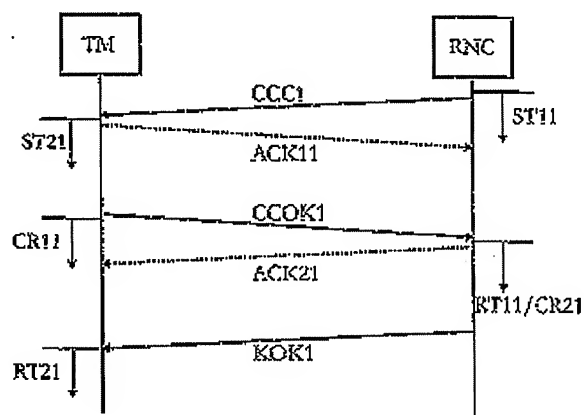
最終頁に続く

(54) 【発明の名称】 暗号鍵交換手順を有する無線ネットワーク

(57) 【要約】

【課題】 本発明の目的は、異なる暗号変更手順を有する無線ネットワークを提供することである。

【解決手段】 本発明は、トラフィック及び、制御チャネルを介して伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ変更するために設けられた、無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークに関する。無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号鍵変更に関するメッセージを端末へ伝送する。端末は、新たな暗号鍵の受取通知として、新たな暗号鍵で符号化されたメッセージで無線ネットワーク制御装置へ応答する。



【特許請求の範囲】

【請求項1】 伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ特定のときに変更するために設けられた、無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークであって、

無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号鍵変更に関するメッセージを端末へ伝送するために設けられ、且つ、

端末は、新たな暗号鍵の受取通知として、新たな暗号鍵で符号化されたメッセージを無線ネットワーク制御装置へ伝送するために設けられたことを特徴とする無線ネットワーク。

【請求項2】 無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号変更命令を端末に送信するようになされ、かつ、

端末は、新たな暗号鍵で符号化された暗号変更命令を無線ネットワーク制御装置に送信するようになされることを特徴とする請求項1記載の無線ネットワーク。

【請求項3】 無線ネットワーク制御装置により送信される暗号変更命令は、新たな暗号鍵を含むことを特徴とする請求項1記載の無線ネットワーク。

【請求項4】 無線ネットワーク制御装置は、受信した鍵が送信した鍵と一致するときには、一致命令を端末へ送信するようになされたことを特徴とする請求項3記載の無線ネットワーク。

【請求項5】 端末が一致命令又は新たな暗号鍵で符号化されたデータを受信したときには、端末は、データの符号化のために無線ネットワーク制御装置から受信した鍵を使用するために設けられていることを特徴とする請求項4記載の無線ネットワーク。

【請求項6】 無線ネットワーク制御装置は、暗号変更の開始時に、データユニットの伝送の停止が成されることを特徴とする請求項1記載の無線ネットワーク。

【請求項7】 新たな暗号鍵の有効性の期間に関するメッセージが交換された後、無線ネットワーク制御装置は、少なくとも1つの端末が新たな暗号鍵を使用しているか否かを確認し、確認後に、新たな暗号鍵又は古い暗号鍵での確認結果に基づき、データユニットの伝送を開始することを特徴とする請求項6記載の無線ネットワーク。

【請求項8】 無線ネットワーク制御装置と少なくとも1つの端末は、データユニット番号を蓄積し且つ同期フェーズ中にデータユニットで使用される鍵を特徴とし、同期フェーズは、無線ネットワーク制御装置又は端末のいずれかからの新たな暗号鍵で符号化された最初のデータユニットの送信と共に開始し、且つ、無線ネットワーク制御装置又は端末のいずれかからの古い暗号鍵で符号化された最後のデータユニットの繰返された送信と共に終了することを特徴とする請求項1記載の無線ネットワ

ーク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、伝送されるべき特定のデータを符号化しかつ特定の時に符号化のために必要な暗号鍵をそれぞれ変更するために設けられた、無線ネットワーク制御装置と複数の割り当てられた端末を含む無線ネットワークに関する。

【0002】

【従来の技術】1992年のVerlag Cell & Sys. Michel Mouly及びMarie-Bernadette Pautetによる「移動通信のためのGMSシステム」391頁から395頁より、データは無線ネットワーク制御装置と端末間で符号化された形式で伝送されることが知られている。伝送に必要な暗号鍵は、特定の時間間隔で変更される。このために3つのステップが設けられる。

【0003】

【発明が解決しようとする課題】本発明の目的は、異なる暗号変更手順を有する無線ネットワークを提供することである。

【0004】

【課題を解決するための手段】この目的は、前文で述べた形式の、無線ネットワーク制御装置は、古い暗号鍵で符号化された暗号鍵変更に関するメッセージを伝送するために設けられ、且つ、端末は、新たな暗号鍵の受取通知として、新たな暗号鍵で符号化されたメッセージを無線ネットワーク制御装置へ伝送するために設けられた無線ネットワークにより達成される。

【0005】本発明に従った無線ネットワークは、複数の無線セルを有し、その中のそれぞれの無線ネットワーク制御装置と複数の端末は、無線で、制御データとペイロードデータを送信する。無線伝送は、例えば、無線、ウルトラシエル又は、赤外線路を介して、情報信号を伝送するために設けられる。

【0006】本発明に従って、端末は新たな暗号鍵で符号化されたメッセージを通知し、そのメッセージは、新たな暗号鍵で符号化されたメッセージ（例えば、暗号鍵命令の受取通知）を送信することによる暗号鍵の変更

（例えば、暗号変更命令）に関する。端末が新たな暗号鍵を間違えて通知されたときには、暗号鍵を受取通知する命令は検出されない。従って、新たな暗号鍵は使用できない。

【0007】

【発明の実施の形態】図1は、例えば、無線ネットワーク制御装置（RNC）1と複数の端末2から9を有するラジオネットワークのような無線ネットワークを示す。無線ネットワーク制御装置1は、例えば、端末2から9のような無線トラフィックに酸化している全構成要素を制御する。制御とペイロードデータの変更は少なくとも

無線ネットワーク制御装置1と端末2から9の間で発生する。無線ネットワーク制御装置1は、ペーロードデータを伝送するためのそれぞれのリンクを確立する。

【0008】 通例として、端末2から9は、移動装置であり、無線ネットワーク制御装置1は、固定されている。無線ネットワーク制御装置1は、移動可能でも良い。

【0009】 無線ネットワークでは、例えば、FDMA（周波数分割多重アクセス）、TDMA（時分割多重アクセス）又は、CDMA（符号分割多重アクセス）法に従った無線信号、又は、それらの方法の結合に従った無線信号が伝送される。

【0010】 特別な符号拡散法であるCDMA法によれば、ユーザからのバイナリ情報（データ信号）は、異なる符号シーケンスで毎回変調される。そのような符号シーケンスは、擬似ランダム矩形波信号（擬似ノイズコード）を有し、そのレートは、チップレートと呼ばれる。擬似ランダム矩形波信号の矩形はパルスの継続時間は、チップ間隔 T_c と呼ばれる。 $1/T_c$ はチップレートである。擬似ランダム矩形波信号とデータ信号の乗算又は、変調はそれぞれ、拡散数 $N_c = T/T_c$ のスペクトラム拡散となる。ここで、 T はデータ信号の矩形パルスの継続時間である。

【0011】 ペーロードデータと制御データは、少なくとも1つの端末（2から9）と無線ネットワーク制御装置1の間で、無線ネットワーク制御装置1により予め定められたチャンネルを介して伝送される。チャンネルは、周波数範囲、時間範囲及び、CDMA方では拡散コードにより決定される。無線ネットワーク制御装置1から端末2から9への無線リンクはダウンリンクと呼ばれ、端末2から無線ネットワーク制御装置1へのリンクはアップリンクと呼ばれる。このように、データは、無線ネットワーク制御装置1から端末2へダウンリンクを介して伝送され、また、端末2から無線ネットワーク制御装置1へはアップリンクを介して伝送される。

【0012】 ダウンリンクチャンネルが設けられ、接続設定に先立ち、無線ネットワーク制御装置1から端末2から9へ制御データを放送するのに使用される。そのようなチャンネルは、ダウンリンク放送制御チャンネルと呼ばれる。接続設定に先立ち、端末2から9から無線ネットワーク制御装置1へ制御データを送信するために、無線ネットワーク制御装置1に割り当てられているアップリンク制御チャンネル使用できるが、しかし、それは、他の端末2から9によってもアクセスされる。種々の又は全ての端末2から9により使用されるアップリンクチャンネルは、共通アップリンクチャンネルと呼ばれる。例えば、端末2から9と無線ネットワーク制御装置1の間の接続の設定後に、ペーロードデータは、ダウンリンク又は、アップリンクユーザチャンネルを介して伝送される。ただ1つの送信器と1つの受信器間で設定されるチャンネルは専

用チャンネルと呼ばれる。通例として、ユーザチャンネルは、リンクに特定の制御データを伝送するための専用の制御チャンネルに関連する専用のチャンネルである。

【0013】 端末2から9を無線ネットワーク制御装置1内に有するために、信号化されたRACHチャンネル（ランダムアクセスチャンネル）と呼ばれる、競合チャンネルは十分である。データパケットは、そのような信号化されたRACHチャンネル上で伝送され得る。

【0014】 ペーロードデータを無線ネットワーク制御装置1と端末間で交換することができるためには、端末2から9は、無線ネットワーク制御装置1と同期していることが必要である。例えば、FDMAとTDMA法の結合が使用されるGSMシステム（移動通信のためのグローバルシステム）から、好適な周波数範囲の決定の後、データ伝送のシーケンス化内でフレーム同期を助ける。所定のパラメータに基づいて、フレームの時間依存に値が決定（フレーム同期）されることが知られる。そのようなフレームは、TDMA、FDMA及び、CDMA法の場合には、常に、端末と無線ネットワーク制御装置のデータの同期には必要である。そのようなフレームは種々のサブフレームを含み又はいくつかの他の連続するフレームと共にスーパーフレームを形成する。簡単のために、基準フレームとして参照されるフレームは開始されたフレームからである。

【0015】 無線ネットワーク制御装置1と端末2から9の間の無線インターフェースを介した制御データの交換を、図2に示すレイヤモデル又は、プロトコル構造を参照して説明する（例えば、第3世代パートナシッププロジェクト（3GPP）；技術仕様グループ（TS G）RAN；ワーキンググループ2（WG2）；無線インターフェースプロトコル構造；TS25.301 V3.2（1990-10）。レイヤモデルは、3つのプロトコルレイヤを有する。物理レイヤPHY、サブレイヤMACとRLC（図2では種々の形式のサブレイヤRLCを含む）データリンクレイヤと、レイヤRRCである。サブレイヤMACは、媒体アクセス制御のためであり、サブレイヤRLCは、無線リンク制御のためであり、レイヤRRCは無線資源制御のためである。レイヤRRCは端末2から9と無線ネットワーク制御装置1間の通信に責任がある。サブレイヤRLCは、端末2から9と無線ネットワーク制御装置1間の無線リンクを制御するのに使用される。レイヤRRCは、サブレイヤMACとPHYを制御リンク10と11を介して制御する。このように、レイヤRRCはサブレイヤMACとPHYのコンフィギュレーションを制御できる。物理レイヤPHYは、サブレイヤMACへの搬送リンクを提供する。サブレイヤMACは、サブレイヤRLCへ有効な論理接続13を行う。サブレイヤRLCはアクセス点14を介して、アプリケーションにより到達できる。

【0016】 そのような無線ネットワークでは、認証さ

れていない方法により盗聴されることを避けるために安全性と信頼性のために、データは符号化された形式で無線インターフェースを介して伝送される。符号化はデータ接続レイヤ（例えば、レイヤRLC又は、MAC内の）データ接続レイヤで行われる。図3に示すように、データDは符号化マスクMと、排他的論理積機能（XOR）を介して結合され、それにより、符号化データストリームC_{UD}を得る。符号化マスクMは、符号化アルゴリズムに従って動作する符号化機能16内で形成され、そして、入力値として、暗号鍵CKとここでは示していない他のパラメータPを受信する。

【0017】暗号鍵は、無線ネットワーク制御装置1と端末2から9の両方で知られていなければならない。暗号鍵は特定の時点で（例えば、1時間おきに）暗号鍵変更と呼ぶ特別の手順で変更される。

【0018】以下は、5つの異なる暗号鍵変更CKC1からCKC5を示す。図4を参照して、第1の手続CKC1を説明する。第1の手順CKC1では、新たな暗号鍵が特に他の4つの手続CKC2からCKC5へ共に送信される。最初に無線ネットワーク制御装置1（図1ではRNCと参照される）は、各端末へのデータの送信（ダウンリンク）を停止する。そのデータは、符号化される（ST11）。1つの例外は暗号鍵変更命令CCC1であり以後説明する。受信されたアップリンクデータは、更に有効な暗号鍵でマスクが解除される。そして、無線ネットワーク制御装置1（RNC）は、端末（図4で、TMとして参照）へ、新たな暗号鍵と共に暗号鍵変更命令CCC1を信号チャネルを介して送る（古い暗号鍵で符号化されている）。安全に関し、変更CKCに先立ち伝送され且つ古い暗号鍵で符号化されるがしかし通知されずに（通知なしのまま）、変更CKC1後に新たにされた伝送があるときに新たな暗号鍵でデータが符号化されるか否かは重要でない。

【0019】端末が新たな暗号鍵と共に暗号鍵変更命令CCC1を受信後、1つの受取通知命令ACK11のみが無線ネットワーク制御装置1に転送され、それにより、所定の時間期間経過後、無線ネットワーク制御装置1は新たな暗号鍵と共に暗号鍵変更命令CCC1を再び送信しない。符号化されるべき各データの転送（アップリンク）も、端末（ST21）により停止される。唯一の例外は以下に説明するような古い暗号鍵で符号化された暗号鍵受取通知命令CCOK1である。それぞれの端末が暗号鍵を暗号鍵変更命令CCC1から取り出し後、端末により暗号鍵変更命令CCC1から取り出された鍵は新たな暗号鍵として登録されそして、暗号鍵受取通知命令CCOK1と共に無線ネットワーク制御装置1へ送信される。暗号鍵受取通知命令CCOK1の送信後、端末はデータを受信し且つ古い暗号鍵と新しい暗号鍵でデータを暗号化する位置にある。古い暗号鍵は、古い暗号鍵で符号化された更新する暗号鍵変更命令CCC1が受

信されたときのみ必要である。これは、例えば、伝送エラーの結果のような暗号鍵受取通知命令CCOK1内に含まれる暗号鍵が元の伝送された暗号鍵と異なるときに起こる。

【0020】暗号鍵受取通知命令CCOK1受信は無線ネットワーク制御装置1により受取通知命令ACK21により端末に通知され、端末へのデータ伝送（ダウンリンク）は新たな暗号鍵と共に回復される。回復は元の伝送された鍵（ST11）が暗号鍵受取通知命令CCOK1内に含まれる鍵と一致するときのみ発生する。受信されたデータは、新たな暗号鍵（CR21）でマスクが解除される。そして、無線ネットワーク制御装置1は、一致命令KOK1を端末に送る。前述のように、暗号鍵変更命令CCC1の送信は暗号鍵が一致しないときは繰り返される。この一致命令KOK1又は、新たな暗号鍵で符号化されたデータ（ダウンリンク）を受信後、端末は新たな暗号鍵（RT21）でデータ伝送（アップリンク）を開始する。これは、手順CKC1を終了指す且つデータ伝送はこの暗号かぎのみで効果がある。

【0021】端末は旧及び新暗号鍵の両方でCR11とRT21間で受信されたデータを解釈するということの結果、端末は、手順CKC1が成功的に終了された（そして端末は古い暗号鍵で符号化された一致命令KOK1を受信する）か、又は、手順は新たに開始されるべきか（この場合には端末は例えば、新たな暗号鍵を再び含む暗号鍵変更命令CCC1を受信する）を認識する。これは、間違って受信された鍵の結果として、端末とネットワーク間の全ての接続が壊されるのを避ける。

【0022】第1の例の上述の手順CKC1は、信号リンクにのみ関連する。データ伝送の繰返しと共に動くデータリンクは、それぞれのレイヤRLCも停止命令（端末：ST21、ネットワークST11）、又は、ペイロードデータの伝送を回復する命令（端末RT21、ネットワークST21）が通知される手順中に含まれる。

【0023】第2の暗号鍵変更CKC2を図5を参照して以下に説明する。この変更CKC2と共に、端末（TM）は別のデータ変更手順（図示していない）内で新たな暗号鍵に関する情報を受信する。暗号鍵自身が無線インターフェースで伝送されることが避けられる。この変更CKC2で、古い暗号鍵から新たな暗号鍵への同期した変更が端末と無線ネットワーク制御装置1（RNS）間で行われる。最初に、符号化されたデータの端末への各伝送（ダウンリンク）は、無線ネットワーク制御装置1（ST21）により停止される。唯一の例外は、以下に説明する暗号鍵変更命令CCC2である。受信されたアップリンクデータは、これまでに使用された暗号鍵でさらに符号化される。そして、（古い暗号鍵で符号化された）暗号鍵変更命令CCC2は、無線ネットワーク制御装置1により信号チャネルを介して端末へ伝送される。安全に関し、変更CKC2に先立ち伝送され且つ古い

暗号鍵で符号化されるがしかし通知されずに（通知なし）のままで、変更CCK2後に新たにされた伝送があるときに新たな暗号鍵でデータが符号化されるか否かは重要でない。

【0024】端末が新たな暗号鍵と共に暗号鍵変更命令CCC2を受信後、1つの受取通知命令ACK12のみが無線ネットワーク制御装置1に転送され、それにより、所定の時間期間経過後、無線ネットワーク制御装置1は新たな暗号鍵と共に暗号鍵変更命令CCC2を再び送信しない。符号化されるべき各データの転送（アップリンク）も、端末（ST22）により停止される。唯一の例外は以下に説明するような新たな暗号鍵で符号化された暗号鍵受取通知命令CCOK2である。暗号鍵受取通知命令CCOK2の伝送後、端末は古い及び新しい暗号鍵の両方でデータを受信し且つ解読（CR12）する。暗号鍵変更命令CCC2が送信されかつ、受取通知命令ACK12が受信された後、無線ネットワーク制御装置1は、新しい暗号鍵と古い暗号鍵の両方でデータを解読する準備がされている。端末は符号化に間違った新たな暗号鍵を使用したために、無線ネットワーク制御装置1内でのこの命令の解読は有益なないようを提供しない（即ち、無線ネットワーク制御装置は、疑いなしに暗号鍵受取通知命令CCOK2であることを認識できない）場合には、無線ネットワーク制御装置1は端末は誤った新たな暗号鍵が通知されることを認識し得る。古い暗号鍵を伴うこの暗号鍵受取通知命令CCOK2の解読は、同様に有益な内容を生じない。この第2の誤った符号化結果は、無線ネットワーク制御装置にとって、端末が誤った新たな暗号鍵を知るといふ更なる確実性を与える。

【0025】暗号鍵受取通知命令CCOK2の受信は、無線ネットワーク制御装置1により受取通知命令ACK22により端末へ通知される。一方、新たな暗号鍵でのCCOK2の解読は、CCOK2が受信されたことを示し、無線ネットワーク制御装置1は再び新たな暗号鍵で、端末とデータ伝送（ダウンリンク）を行う（RT12）。受信されたデータは新たな暗号鍵のみでマスクが解除される。無線ネットワーク制御装置1は、端末に新たな暗号鍵で符号化された一致命令KOK2を送る。

【0026】暗号鍵受取通知命令CCOK2が（上述のように）解読できない場合には、再び、古い暗号鍵が受信と送信の両方で使用される（RT12/CR22）。そして、無線ネットワーク制御装置1は、古い暗号鍵で符号化された一致命令KOK2を端末へ送る。この後無線ネットワーク制御装置1は有効なら、他のデータの伝送を回復する。

【0027】端末と無線ネットワーク制御装置に既知の新たな暗号鍵で暗号の変更を可能とするために、RLCレイヤはデータ交換手順を行う管理レイヤに知らせ、そして、ここでは説明されないが他の新たな暗号が端末へ

通知される。

【0028】この新たな暗号鍵で符号化された一致命令KOK2の受信後、端末は新たな暗号鍵（RT22）でデータ伝送（アップリンク）を開始する。これは手順CCK2を終了させ、データ転送はこの鍵のみで行われる。

【0029】古い暗号鍵で符号化されたこの一致命令KOK2の受信後、端末は古い暗号鍵でデータ伝送（アップリンク）を回復し、そして、新たな暗号鍵の同時受信が終了される。これは変更CCK2を破り停止する。

【0030】端末は古い暗号鍵と新たな暗号鍵の両方でCR12とRT22間で受信されたデータを解読するので、端末は、手順CCK2が成功的に終了された（そして端末は新たな暗号鍵で符号化された一致命令KOK2を受信し、かつ新たな暗号鍵で解読することは、一致命令KOK2が適することを生じ、一方古い暗号鍵で解読することは有益な内容を生じない）か、又は、新たな暗号鍵に変更後の手順は新たに開始されるべきか（そして、端末は古い暗号鍵で符号化された一致命令KOK2を受信する；ここで新たな暗号鍵で解読することは有益な内容を生じず、一方、古い暗号鍵で解読することは、KOK2が適することを生じるを認識する。これは、間違っ受信された鍵の結果として、端末とネットワーク間の全ての接続が遮断されるのを避ける。

【0031】上述の変更CCK2は最初に信号リンクにのみ関連する。データ伝送の繰返しと共に働くデータリンクは、それぞれのレイヤRLCが停止命令（端末：ST22、ネットワークST12）、又は、ペイロードデータの伝送を回復する命令（端末RT12、ネットワークCR22）が通知される変更中に含まれる。

【0032】メッセージがレイヤRLCとレイヤRRC間で伝送される第3の変更CCK3を図6から8を参照して説明する。レイヤRLCでは、更に自分及び、インスタンスRLC（DC）とRLC（DT）間でメッセージが交換される。インスタンスRLC（DT）は、専用トラフィックチャネル（DTCCH）に対してであり、インスタンスRLC（DC）は専用制御チャネル（DCCCH）に関してである。

【0033】暗号鍵変更CCK3とともに、無線ネットワーク制御装置1は端末2から9へ新たな暗号鍵の有効性を通知する。この新たな暗号鍵は、無線ネットワーク制御装置1と端末2から9の両方に既知である。図6から8は、端末のレイヤRRCとRLC（"T"として参照する図6から8の左側）と、無線ネットワーク制御装置1（"F"として参照する図6から8の右側）間で送られる種々のメッセージを示す。以後説明する図6は暗号鍵変更CCK3の始まりを示す。暗号鍵変更CCK3は、サイドFのレイヤRRCによりローカルメッセージCRLC-S-R（ND）により開始される。ローカルメッセージと共にインスタンスRLC（DC）は、デー

10

20

30

40

50

タユニット中のシリアル番号SN（各データユニットはシリアル番号が付される）が $SN \geq VTD + ND$ の条件を満たす限りメッセージ中のデータユニットの伝送は停止されたことを通知される。ローカルメッセージCRLC-S-R(ND)のパラメータNDは、そして、まだ伝送されるべきデータユニットの数を示し、そして、VYDはRLC(DC)で既知の伝送されるべき次のデータユニットのシリアル番号を示す。ローカルメッセージCRLC-S-R(VTD)により、サイドFのインスタンスRLC(DC)は、シリアル番号NDの受信を知らせ、且つレイヤへ番号VTDを知らせる。続いて、サイドFのレイヤRRCは、インスタンスRLC(DC)にローカルメッセージCRLC-CONF-R(CKN)を介して使用されるべき新たな暗号鍵CKNを知らせる。このメッセージは、ローカルメッセージCRLC-CONF-Cを介してRLC(DC)により通知される。

【0034】インスタンスRLC(DC)のレイヤRRCが、ローカルメッセージRLC-AM-DAT-Rを配送後、サイドFのインスタンスRLC(DC)は、メッセージSEC-MO-COM(VTD, ND)をサイドT(端末)のインスタンスRLC(DC)へ送る。このメッセージは、安全モード命令を示し、これまで有効な古い暗号鍵で符号化される。メッセージは、番号VTDとNDを伴うデータユニットを含む。メッセージの受信後、サイドTのレイヤRRCのインスタンスRLC(DC)は、ローカルメッセージRLC-AM-DAT-Iを介して、有効であるべき新たな暗号鍵が有効なときから、指示を有するメッセージが到着したことを示す。この新たな暗号鍵は解読を保持する。それはデータユニットのシリアル番号VTD+ND後である。サイドTのインスタンスRLC(DC)で、メッセージSEC-MO-COM(VTD, ND)の受信は、命令ACKを介してサイドFのインスタンスRLC(DC)から通知され、そして、更にレイヤRRCからローカルメッセージRLC-AM-DAT-Cを介して通知される。このように無線ネットワーク制御装置1は、端末は暗号鍵変更の最初で通知され且つ条件 $SN \geq VTD + ND$ を満たすシリアル番号SNのデータユニットを解読するのに新たな暗号鍵を使用することが通知される。

【0035】サイドT(端末)からの開始で、同様なメッセージの交換が関係のレイヤ間で行われる。サイドTのレイヤRRCからのローカルメッセージCRLC-S-R(NU)は、サイドTからのメッセージの交換を開始する。メッセージと共に、条件 $SN \geq VTD + NU$ を満たすシリアル番号SNのデータユニットの伝送は、停止される。インスタンスRLC(DC)は更に伝送されるべきデータユニットの番号NUが通知される。ローカルメッセージCRLC-S-C(VTD)により、サイドTのインスタンスRLC(DC)は番号NUの受信を

通知し、且つレイヤに番号VTDを示す。ローカルメッセージCRLC-S-C(VTD)の受信後（アップリンクで）最初に送られるこの番号VTUデータユニットのシリアル番号SNを示す（繰返し伝送はない）。続いて、サイドTのレイヤRRCは、インスタンスRLC(DC)へローカルメッセージCRLC-CONF-R(CKN)を介して鍵を変更することを望むことを知らせる。このメッセージはローカルメッセージCRLC-CONF-Cを介してサイドTのインスタンスRLC(DC)へ通知される。

【0036】ローカルメッセージRLC-AM-DAT-Rを介して、サイドTのレイヤRRCから、インスタンスRLC(DC)へ、新たな暗号鍵がサイドTに関して保つときからを示す暗号鍵変更部分が開始される。ローカルメッセージRLC-AM-DAT-Rが受信された後、サイドT(端末)のインスタンスRLC(DC)は、メッセージSEC-MO-CMPL(VTU, NU)をサイドF(無線ネットワーク制御装置)のインスタンスRLC(DC)へ送る。このメッセージは、安全モード命令を示し、これまで有効な暗号鍵と共に符号化される。メッセージは番号VTUとNUを有するデータユニットを含む。このメッセージの受信後、サイドFのレイヤRRCのインスタンスRLC(DC)は、ローカルメッセージRLC-AM-DAT-Iを介して、メッセージが無線ネットワーク制御装置1内で解読のために新たな暗号鍵が有効となるべきときから到着したときを示す。この新たな暗号鍵はデータユニットのシリアル番号VTU+NU後に有効である。サイドFのレイヤRLCで、メッセージSEC-MO-CMPL(VTU, NU)の受信は、サイドFのインスタンスRLC(DC)の命令ACKを介して通知され、そして、更にローカルメッセージRLC-AM-DAT-Cを介してレイヤRRCへ通知される。このように、無線ネットワーク制御装置1は端末がシリアル番号VTU+NUから開始する自身のメッセージのデータユニットを符号化するために新たな暗号鍵を使用することを知っていることが端末に知らされる。

【0037】図7はプロローグに続いた第1のテスト部分として示される手続の更なる部分を示す。この部分の間は、新たな暗号鍵で符号化された2つのサイドTとFのデータユニットからのメッセージ内で正しく符号化され認識される。第1のテスト部分はローカルメッセージCRLC-CONF-R(VTU+NU)で開始し、それは、レイヤRRCからインスタンスRLC(DC)へサイドFで伝送される。このように、次のデータユニットのシリアル番号SNに対して $SN \geq VTU + NU$ 又は、 $SN = VR$ の条件が成り立つときには、インスタンスRLC(DC)は端末から受信された全てのメッセージは新たな暗号鍵で解読されるべきであることが通知される。ここで、VRは最初に伝送される次の予想される

データユニットを示す。インスタンスRLC(DC)は、レイヤRRCヘローカルメッセージCRLC-CONF-Cを送ることによりローカルメッセージCRLC-CONF-R(VTU+NU)の受信を通知する。サイドTでは、インスタンスRLC(DC)は、レイヤRRCからインスタンスRLC(DC)ヘローカルメッセージCRLC-CONF-R(AP)を伝送することにより、このメッセージ後、サイドF(無線ネットワーク制御装置1)で伝送されるべき以下のデータユニットが新たな暗号鍵で符号化されることが通知される。しか

し、サイドFの受信されたメッセージは、まだ、古い暗号鍵で解読されるべきである。インスタンスRLC(DC)は、サイドTのレイヤRRCヘローカルメッセージCRLC-CONF-R(AP)の受信を通知する。
 【0038】以下のメッセージルーチンと共に、2つのサイドTとFが同じ新たな暗号鍵を使用するか否かがチェックされる。このメッセージルーチンはサイドFのレイヤRRCによりインスタンスRLC(DC)へのローカルメッセージRLC-AM-DAT-Rと共に開始される。このメッセージと共に、サイドFのインスタンスRLC(DC)古い暗号鍵で符号化されたメッセージSCKCをサイドTのインスタンスRLC(DC)へ送るように要求される。このメッセージSCKCの受信後、サイドTのインスタンスRLC(DC)は、サイドFのインスタンスRLC(DC)へ受信の通知ACKを送る。サイドTのレイヤRRCは、サイドTのインスタンスRLC(DC)へ、ローカルメッセージRLC-AM-DAT-R内のメッセージN(CKCC)を送る。そのメッセージは、サイドTのインスタンスRLC(DC)により複数のデータユニットに分割される。サイドTのインスタンスRLC(DC)は、新たな暗号鍵でこれらのデータを符号化し、そして、サイドFのインスタンスRLC(DC)へそれら(図7のメッセージCKCC)を送る。サイドFのインスタンスRLC(DC)は新たな暗号鍵でメッセージCKCCの全ての受信したデータユニットを解読し、メッセージCKCC内で送信されたデータユニットからのメッセージN(CKCC)を構築し、そして、サイドFのレイヤRRCへ、ローカルメッセージRLC-AM-DAT-I*内でこのメッセージN(CKCC)を転送する。ローカルメッセージRLC-AM-DAT-I*は、ローカルメッセージCRLC-CONF-R(VTU+NU)の受信後、最初のデータユニットがシリアル番号SN=VR(これは正確にメッセージCKCCである)を有するなら、メッセージN(CKCC)に関してのみ使用される。この結果、サイドFのレイヤRRCはインスタンスRLC(DC)からメッセージN(CKCC)を得ることを知る。

【0039】サイドTで、正しい新たな暗号鍵が使用される場合には、サイドのレイヤRRCは、ローカルメッ

セージRLC-AM-DAT-I*内に期待するメッセージN(CKCC)を受信する。間違った新たな暗号鍵がサイドTで使用される場合にはサイドFのレイヤRRCは、ローカルメッセージRLC-AM-DAT-I*内に、使用できない又は知られていないメッセージを受信する。サイドFのレイヤRRCは、それから、サイドTは、間違った鍵を使用した即ち、この特定の場合には知られていないメッセージは無視されないと推定する。

【0040】メッセージCKCCの受信後、サイドFのインスタンスRLC(DC)は、サイドTのインスタンスRLC(DC)へ、命令ACKを介してメッセージCKCCの受信を通知する。受信はサイドTのインスタンスRLC(DC)により、ローカルメッセージRLC-AM-DAT-Cを介してレイヤRRCへ転送される。

【0041】メッセージRLC-AM-DAT-I*内に含まれている通信を受信後、サイドFのレイヤRRCはTのレイヤRRCへ、サイドTは正しい新たな暗号鍵を使用したか間違った新たな暗号鍵を使用したか(CKST=暗号鍵状態)についての指示を含む、通信N(CKST)を送る。サイドFのレイヤRRCは、ローカルメッセージRLC-AM-DAT-R内の通信N(CKST)をサイドFのインスタンスRLC(DC)へ与るので、これは、順番に起こる。それは、通信を複数のデータユニットに分割し、古い暗号鍵で符号化され、メッセージCKSTを介してサイドTのインスタンスRLC(DC)へ送る。サイドTのインスタンスRLC(DC)は、メッセージACKを介してこちらのデータユニットの受信を通知し、それらを古い暗号鍵で解読し、そして、通信N(CKST)を再び再構築する。この通信N(CKST)はローカルメッセージRLC-AM-DAT-I*内でサイドTのレイヤRRCへ送られる。

【0042】サイドTで、正しい新たな暗号鍵が使用される場合には、サイドFのレイヤRRCは、ローカルメッセージCRLC-RES-Rを介してインスタンスRLC(DC)へ、新たな暗号鍵を使用しながらデータユニットの伝送を再開することを命じる。サイドFでの解読は受信データユニットのシリアル番号が、 $SN \geq VTU + NU$ 成り立つときには、新たな暗号鍵で行われる。

【0043】メッセージCKSTがサイドTで使用された新たな暗号鍵が正しいという通知を含む場合には、サイドTのレイヤRRCは、ローカルメッセージCRLC-RES-Rを介してインスタンスRLC(DC)へ、新たな暗号鍵を使用しながら再びデータユニットの伝送を開始することを命じる。サイドTでの解読は、受信データユニットのシリアル番号に、 $SN \geq VTU + NU$ 成り立つときには(図7)、新たな暗号鍵で行われる。

【0044】サイドTで、誤った新たな暗号鍵が使用されたときには(誤った鍵に対する最初のチェック部を示す図8と比較する)、サイドFのレイヤRRCは、ローカルメッセージCRLC-CONF-Rを介してサイド

FのインスタンスRLC(DC)へ、条件 $SN \geq VTU + NU$ 成り立つときには、解読のための新たな暗号鍵への変換はキャンセルされたことを命じる。伝送が停止されるデータユニットの符号化に対しては、再び古い暗号鍵が使用される。ローカルメッセージCRLC-CONF-Rは、ローカルメッセージCRLC-CONF-Cを介してインスタンスRLC(DC)により通知される。ローカルメッセージCRLC-RES-Rにより、サイドFのレイヤRRCは、インスタンスRLC(DC)へデータユニットの伝送の回復を(古い暗号鍵で) 10 通知する。メッセージCKSTがサイドTで使用された新たな暗号鍵が正しくないという支持を含む場合には、サイドTのレイヤRRCは、ローカルメッセージCRLC-CONF-Rを介して、インスタンスRLC(DC)へ、条件 $SN \geq VTD + NU$ 成り立つときには、解読のための新たな暗号鍵への変換はキャンセルされたことを命令し、ローカルメッセージCRLC-CONF-Cにより通知される。データユニットがまだ停止しているデータユニットの符号化に関しては、古い暗号鍵が使用される。ローカルメッセージCRLC-RES-Rにより、 20 サイドFのレイヤRRCは、インスタンスRLC(DC)へデータユニットの伝送を回復することを(古い暗号鍵で)告げる。

【0045】第4の暗号鍵変更手順CKC4を図9から12により説明する。図9と10は、端末が正しい新たな暗号鍵を使用し、又は、端末が誤った新たな暗号鍵を使用する場合のそれぞれの場合を示す。暗号鍵変更手順CKC4を示す。新たな暗号鍵で符号化及び解読への結果の変換に先立ち、端末が正しい新たな暗号鍵を使用するか否かの第1のチェックが行われるので、エラーの場合には、符号化と解読はサイドTとFの間の全ての接続(データ損失なし)が終了されること無く、古い暗号鍵で回復されることができる。以下の手順では、単一の専用のトラフィックチャンネルが信号リンク(DC)に加えて考慮される。従って、一般的には、手順を拡張する、複数の専用のトラフィックチャンネルと(手順CKCのシグナリング目的に使用されない)異なる専用の制御チャンネルが可能である。

【0046】暗号鍵変更手順CKC4(図9)は、ローカルメッセージCRLC-S-R(ND_DC)又は、 40 CRLC-S-R(ND_DT)を介してそれぞれサイドFのレイヤRRCからインスタンスRLC(DC)又は、RLC(DT)へ開始される。ローカルメッセージCRLC-S-R(ND_DC)又は、CRLC-S-R(ND_DT)を介してそれぞれ、インスタンスRLC(DC)又は、RLC(DT)それぞれは、これまで、データユニットのシリアル番号(各データユニットにはシリアル番号が付される)が、条件 $SN \geq VTD_DC + ND_DC$ 又は、 $SN \geq VTD_DT + ND_DT$ を満たす場合にはデータユニットの伝送が停止される 50

ことが通知される。そして、ローカルメッセージCRLC-S-R(ND_DC)又は、CRLC-S-R(ND_DT)のパラメータND_DCとND_DTはそれぞれ、まだ送信されるべきデータユニットの数を示し、且つ、VTD_DCとVTD_DTはそれぞれ、最初に伝送されるべき告ぎのデータユニットのRLC(DC)又は、RLC(DT)内で既知のシリアルある番号SNである。制御チャンネルDCに関しては、選択されたND_DCは少なくとも非常に大きいので、続くダウンリンクメッセージSEC-MO-CNDとSEC-MO-KC(図9と10)の全データユニットは、伝送が停止される前に更に送信される。トラフィックチャンネルND_DTはゼロの設定される。

【0047】ローカルメッセージCRLC-S-R(ND_DC)又はCRLC-S-R(ND_DT)それぞれによって、サイドFのインスタンスRLC(DC)又はRLC(DT)はそれぞれ、番号ND_DC又はND_DTの受信を通知し、且つ番号VTD_DC又はVTD_DTをレイヤに知らせる。続いて、サイドFのレイヤRRCは、インスタンスRLC(DC)又はRLC(DT)それぞれに、ローカルメッセージCRLC-CONF-R_DC(CKN)又はCRLC-CONF-R_DT(CKN)を介して、使用されるべき新たな暗号鍵CKNを通知する。このメッセージはサイドFのインスタンスRLC(DC)又はRLC(DT)それぞれにより、ローカルメッセージCRLC-CONF-C_DT又はCRLC-CONF-C_DCを介して、通知される。

【0048】サイドFのインスタンスRLC(DC)は、レイヤRRCから受信されたローカルメッセージRRC-DAT-R内に含まれる通信SEC-MO-CNDをサイドTのインスタンスRLC(DC)へ送る。この通信は、安全モード命令を示し、古い今まで有効な鍵で符号化される。1つ又はそれ以上のデータユニットを含む通信は番号VTD_DC, ND_DC, VTD_DT及び、VTD_DTを含む。

【0049】通信の受信後、サイドTのレイヤRRCのインスタンスRLC(DC)は、ローカルメッセージRLC-AM-DAT-Iを介して、この通信は新たな暗号鍵が有効となるべきときからの指示を有して到着したことを指示する。この新たな暗号鍵は、データユニットのシリアル番号VTD_DC+ND_DCから解読するために制御チャンネルDC上で前方へ有効であり、シリアル番号VTD_DT+ND_DTからのトラフィックチャンネル上で前方へ有効である。サイドTのインスタンスRLC(DC)通信SEC-MO-CMDの受信は、サイドのインスタンスRLC(DC)の受信通知ACKを介して、通知され、且つ更に、ローカルメッセージRLC-AM-DAT-Cを介してさらにレイヤRRCへ通知される。このように、無線ネットワーク制御装置1に

は、制御チャンネルの場合にはシリアル番号SNが条件 $SN \geq VTD_DC + ND_DC$ を満たし、トラフィックチャンネルの場合にはシリアル番号SNが条件 $SN \geq VTD_DT + ND_DT$ を満たすときには、端末が暗号鍵変更手順の開始が通知されデータユニットの解読に新たな暗号鍵が使用されるということが、知られている。

【0050】上述のローカルメッセージCRLC-CONF-R_DC (CKN) とCRLC-CONF-R_DT (CKN) それぞれにより、サイドFのレイヤRRCはインスタンスRLC (DC) 又はRLC (DT) それぞれに、新たな暗号鍵で全ての新たな即ち、繰返しとして送られない期待されるデータユニットを(次の通信が完了するまで) 符号化することを命じる。それらは、上述のローカルメッセージCRLC-CONF-R_DC (CKN) とCRLC-CONF-R_DT (CKN) の受信時にシリアル番号が条件 $SN \geq VR$ を満たすデータユニットである。ここで、VRはインスタンスRLC (DC) で変数であり、次の予想されるデータユニットは繰返しとして送信されないシリアル番号を意味する。

【0051】サイドT (端末) (図10) の開始からそれぞれのレイヤ間の同様なメッセージの交換が行われる。ローカルメッセージCRLC-S-R (ND_DC) からインスタンスRLC (DC) 又は、CRLC-S-R (ND_DT) からインスタンスRLC (DT) それぞれ、サイドTのレイヤRRCからサイドTから来るメッセージの交換が開始する。これらの2つのローカルメッセージで、番号が条件 $SN \geq VTD_DC + ND_DC$ (制御チャンネルに対して) 及び、 $SN \geq VTD_DT + ND_DT$ (トラフィックチャンネルに対して) を満たすデータユニットの伝送は停止される。そして、まだ伝送されるべきデータユニットの番号NU_DC又は、NU_DTは、インスタンスRLC (DC) 又はRLC (DT) へそれぞれ通知される。制御チャンネルDCに関しては、NU_DCは(少なくとも) 大きく選択されるべきなので、以下のアップリンク通信SEC-MO-KC (図10) とSEC-MO-CMPLそれぞれ (図11と12) は伝送が停止される前に送られる。トラフィックチャンネルNU_DTに関してはゼロに設定される。

【0052】ローカルメッセージCRLC-S-C (VTU_DC) 又はCRLC-S-C (VTU_DT) により、サイドTのインスタンスRLC (DC) 又はRLC (DT) それぞれは、番号NU_DC又は、NU_DTの受信をそれぞれ通知され、そして、レイヤに、番号VTU_DC又はVTU_DTをそれぞれ示す。この番号VTU_DC又はVTU_DTは、それぞれローカルメッセージCRLC-S-C (VTU_DC) 又はCRLC-S-C (VTU_DT) の受信後に、制御チャンネル又は、アップリンク内のトラフィックチャンネル(繰返

し伝送なし) を介して、最初に送信されるデータユニットのシリアル番号SNを示す。続いて、サイドTのレイヤRRCは、インスタンスRLC (DC) 又はRLC (DT) それぞれにローカルメッセージCRLC-CONF-R_DC (CKN) 又は、CRLC-CONF-R_DT (CKN) を介して、それぞれ、暗号鍵の変更の希望を通知する。番号VTD_DC+ND_DCにより、VTD_DT+ND_DTは、さらに、そこから前方へ新たな暗号鍵で解読が行われる。データユニットのシリアル番号が通知される。各々がローカルメッセージCRLC-CONF-C_DC又はCRLC-CONF-C_DTを伴う、このローカルメッセージは、サイドTのインスタンスRLC (DC) 又はRLC (DT) により通知される。

【0053】インスタンスRLC (DC) へのサイドTのレイヤRRCのローカルメッセージRLC-AM-DAT-R*により、手順部分は開始し、それによりサイドFは、サイドTは正しい新たな暗号鍵を使用するか否かをチェックできる。ローカルメッセージRLC-AM-DAT-R*の受信後、サイドT (端末) のインスタンスRLC (DC) は、通信SEC-MO-KCをサイドF (無線ネットワーク制御装置1) のインスタンスRLC (DC) へ送り、新たな暗号鍵で符号化される。上記場合のアスタリスク ("*") は、(例えば、ローカルメッセージRLC-AM-DAT-R内の異なるパラメータ(フラグ)により)、インスタンスRLC (DC) が、この特定の通信に対して符号化に新たな暗号鍵が使用されるべきであることが示されていることを意味する。

【0054】サイドFのインスタンスRLC (DC) でメッセージのデータユニットのシリアル番号が条件 $SN \geq VR$ を満たし、それによりそれらは新たな暗号鍵で解読される。新たな暗号鍵で解読されたデータユニットからの再構成されたメッセージは、ローカルメッセージRLC-AM-DAT-I*と共にサイドFのレイヤRRCへ与えられ、一方上記場合のアスタリスク ("*") は、(例えば、ローカルメッセージRLC-AM-DAT-I内の異なるパラメータ(フラグ)により)、RRCが、パラメータとして伝送された通信が新たな暗号鍵で解読されるデータユニットの組合せであることを示されることを意味する。正しい鍵の信頼あるチェックのために、通信SEC-MO-KCに、複数のデータユニットよりなることが必要である。

【0055】サイドFのレイヤRRCはこの時点で通信SEC-MO-KCを期待する。サイドTで正しい新たな暗号鍵が符号化に使用される場合には、レイヤRRCはローカルメッセージRLC-AM-DAT-I*のパラメータ内のこの通信を認識し、且つ図10と11に記載されたように手順が行う。

【0056】サイドTで新たな間違った暗号鍵が符号化

10

20

30

40

50

に使用される場合には、レイヤRRCはローカルメッセージRLC-AM-DAT-I*のパラメータ内の通信は有益又は既知でないと認識する。この特定の場合、知られていない通信がローカルメッセージRLC-AM-DAT-I*と共にレイヤRRCにより受信された場合には、レイヤRRCはこの知られていない通信を単純に拒絶せず、しかし、サイドTは間違った新たな暗号鍵を使用していると認識する。この場合は、手続は図12に示すように継続する。

【0057】両場合には、サイドFのレイヤRRCは（インスタンスRLC(DC)へのローカルメッセージRLC-AM-DAT-Rのパラメータとして）、サイドTで、通信SEC-MO-KCSTを送る。それは、サイドFのレイヤRRCが確立されたか否か、サイドTは正しい新たな暗号鍵又は誤った新たな暗号鍵を使用しているかの指示を含む。通信SEC-MO-KCSTのデータユニットは、常に古い暗号鍵で符号化される。

【0058】以下は図11に示す通常の場合である。サイドFのインスタンスRLC(DC)へ、サイドFの通信SEC-MO-KCSTの受信に関して、サイドTのインスタンスRLC(DC)により受信の通知ACKを転送する。ローカルメッセージRLC-AM-DAT-Cの受信後、サイドFのレイヤRRCはローカルメッセージCRLC-RES-R_DC又はCRLC-RES-R_DTを介して、インスタンスRLC(DC)又はRLC(DT)へ、インスタンスRLC(DC)内のシリアル番号SNが条件 $SN \geq VTD_DC + ND_DC$ を満たし又は、インスタンスRLC(DT)内で条件 $SN \geq VTD_DT + ND_DT$ を満たす今まで停止されていたデータユニットの伝送を開始するように命じる。これらのデータユニットは新たな暗号鍵で符号化される。

【0059】以下の図12に示すエラーの場合が記述される。レイヤRRCへ、サイドFの通信SEC-MO-KCSTの受信に関して、サイドTのRLC(DC)の受信の通知ACKを転送する。ローカルメッセージRLC-AM-DAT-Cが受信された後、サイドFのレイヤRRCは以後説明する更なるメッセージの後に、最初にローカルメッセージCRLC-CONF-R_DC又はCRLC-CONF-R_DTそれぞれにより、ローカルメッセージCRLC-CONF-C_DC又CRLC-CONF-C_DTにより通知される、新たな暗号鍵の変換をキャンセルすることを命じ、続いてローカルメッセージCRLC-RES-R_DC又はCRLC-RES-R_DTにより、レイヤRLC(DC)内のシリアル番号SNが、条件 $SN \geq VTD_DC + ND_DC$ 又は、RLC(DT)内のシリアル番号SNが、条件 $SN \geq VTD_DT + ND_DT$ を満たす今まで停止してデータユニットの伝送を回復することを命じる。これらのデータユニットは古い暗号鍵で符号化される。

【0060】受信の通知ACKの結果、サイドFの通信SEC-MO-KCの受信はT(図10)へ通知される。ローカルメッセージRLC-AM-DAT-Cはこの通知をサイドT上のレイヤRRCへ伝送する。通知の受信後、サイドTはサイドFからの通信SEC-MO-KCSTを期待する(図11及び12)。インスタンスRLC(DC)での通信SEC-MO-KCSTの受信の時は、その受信はサイドFへ通信ACKを介して通知され、サイドTのこのインスタンスは通信SEC-MO-KCSTをローカルメッセージRLC-AM-DAT-IのパラメータとしてサイドTのレイヤRRCへ渡す。

【0061】通常の場合(図11)にサイドTの通信SEC-MO-KCSTが使用される新たな暗号鍵が正しい新たな暗号鍵を示す場合には、サイドTは通信SEC-MO-CMPLをサイドFへ送る。ローカルメッセージRLC-AM-DAT-R(図11)の受信後、サイドT(端末)のインスタンスRLC(DC)は通信SEC-MO-CMPLをサイドF(無線ネットワーク制御装置)のインスタンスRLC(DC)へ送る。この通信は安全モード命令を示し、且つそれまで有効な古い暗号鍵で符号化される。メッセージは1つ又はそれ以上のデータユニットからなり、番号VTU_DC, NU_DC, VTU_DT及び、NU_DTを転送する。通信の受信後、サイドFのレイヤRRCのインスタンスRLC(DC)は、ローカルメッセージRLC-AM-DAT-Iを介して、この通信は、無線ネットワーク制御装置内の解読に関して新たな暗号鍵が有効であるべき時からの指示と共に到着したことを示す。この新たな暗号鍵は、シリアル番号SNが、条件 $SN \geq VTU_DC + NU_DC$ (制御チャネル)又は、条件 $SN \geq VTU_DT + NU_DT$ (トラフィックチャネル)を満たすデータユニットを表す。

【0062】通信SEC-MO-CMPLの受信後、FのレイヤRRCはインスタンスRLC(DC)又はRLC(DT)に、ローカルメッセージCRLC-CONF-R_DC又はCRLC-CONF-R_DTにより、シリアル番号SNが、インスタンスRLC(DC)では条件 $SN \geq VTU_DC + NU_DC$ 又は、インスタンスRLC(DT)では条件 $SN \geq VTU_DT + NU_DT$ (トラフィックチャネル)を満たす全てのデータユニットを解読するための新たな暗号鍵を使用することを命じる。

【0063】サイドFのインスタンスRLC(DC)で通信SEC-MO-CMPLは、サイドTのインスタンスRLC(DC)の受信の通知ACKを介して通知され、且つ更に、それらのレイヤRRCはローカルメッセージRLC-AM-DAT-Cを介して通知される。このように、端末には、無線ネットワーク制御装置1には端末が、制御チャネル上のシリアル番号VTU_DC+

NU_DCから前方へ及び、トラフィックチャネル上のVTU_DT+NU_DTから、新たな暗号鍵を自己の通信のデータユニットの符号化に対して使用することを知っているということを知る。

【0064】サイドTは正しい新たな暗号鍵を使用するので、それらのレイヤRRCはインスタンスRLC(DC)又はRLC(DT)へ、ローカルメッセージCRLC-RES-R_DC又はCRLC-RES-R_DT(図11)を介して、ローカルメッセージRLC-AM-DAT-C受信後、シリアル番号SNが、制御チャネルに対してはインスタンスRLC(DC)で条件SN≥VTU_DC+NU_DC又は、トラフィックチャネルに対してはインスタンスRLC(DT)では条件SN≥VTU_DT+NU_DTを満たす今まで停止されたデータユニットの伝送を回復するように命じる。

【0065】サイドTの通信SEC-MO-KCSTが使用される新たな暗号鍵が間違い(誤り)(図12)であることを示すときには、レイヤRRCは、インスタンスRLC(DC)又はRLC(DT)に、2つのローカルメッセージCRLC-CONF-R_DCとCRLC-CONF-R_DTにより、新たな暗号鍵の変換を停止するように命じる。

【0066】さらに、サイドTは通信SEC-MO-CMPLを、サイドFへ手順を終了するために送る。この通信は、ローカルメッセージRLC-AM-DAT-Rのパラメータとして、無線インターフェースを介してサイドFのインスタンスRLC(DC)へ与えられ、このインターフェースによりローカルメッセージRLC-AM-DAT-IのパラメータとしてサイドFのレイヤRRCへ与えられる。新たな暗号鍵の使用は切り替えがつづいていないので、メッセージSEC-MO-CMPLは、番号VTU_DC、NU_DC、VTU_DT及び、NU_DTを含む必要がない。

【0067】解説に関しては、サイドFのインスタンスRLC(DC)又はRLC(DT)でなにも変更が起こらず、解説のためにこれらのインスタンスに関して再コンフィグレーションはいずれも必要で無く、それにより暗号鍵変更CKCは、サイドFのエラーの場合には、通信SEC-MO-CMPLの受信で終了する。

【0068】サイドTのインスタンスRLC(DC)の通信SEC-MO-CMPLに対する受信の通知ACK後、それはサイドTのレイヤRRCへローカルメッセージRLC-AM-DAT-Cを介して伝送される。サイドTのレイヤRRCはそして、インスタンスRLC(DC)又はRLC(DT)へ、2つのローカルメッセージCRLC-RES-C_DC又は、CRLC-RES-C_DTにより、シリアル番号SNが、制御チャネルに対してはインスタンスRLC(DC)で条件SN≥VTU_DC+NU_DC又は、トラフィックチャネルに対してはインスタンスRLC(DT)では条件SN≥

VTU_DT+NU_DTを満たす今まで停止されたデータユニットの伝送を回復するように命じる。

【0069】新たな暗号鍵への変更は前にインスタンスRLC(DC)で2つのローカルメッセージCRLC-CONF-R_DC及びインスタンスRLC(DT)でCRLC-CONF-R_DTを介してキャンセルされているので、これらのデータユニットは、古い暗号鍵で符号化される。エラーの場合には、暗号鍵変更はサイドTで終わる。

10 【0070】第5の暗号鍵変更手順CKC5を13と14により説明する。前述のように、レイヤRLCとレイヤRRC間のローカルメッセージはこの手順中に伝送される。レイヤRLCは2つのインスタンスRLC(DC)又はRLC(DT)を利用できる。インスタンスRLC(DT)は専用トラフィックチャネル(DTCH)を制御でき、非専用インスタンスRLC(DC)は専用制御チャネル(DCCH)を制御できる。端末は例えば、GSM("GSM移動通信のためのグローバルシステム" J. EberspacherとH. J. Vogel, Teubner Stuttgart 1997年146頁から154頁参照)で説明されているように端末と無線ネットワーク制御装置の間の別の貸小手順で新たな暗号鍵についての情報を受信する。この文献中では、鍵

20 それ自身は無線インターフェースを介して伝送される。【0071】記述されるべき手順CKC5で、端末と無線ネットワーク制御装置間の古い暗号鍵から新たな暗号鍵への同期した変換が行われる。手順CKC5は、プロローグフェーズで始まり、同期フェーズが続く。図13と14は、端末のレイヤRRCとレイヤRLC(図4と5の左側を" T "と呼ぶ)と無線ネットワーク制御装置(図4と5の右側を" F "と呼ぶ)間で送られる種々のメッセージを示す。

【0072】最初に、(図4と比較して)無線ネットワーク制御装置1は、端末に新たな暗号鍵の意図された変更を通知する。サイドFでは、レイヤRRCは、インスタンスRLC(DC)へローカルメッセージAMD-REQ-CCCにより通信AMD-PDU-CCCをサイドTのインスタンスRLC(DC)へ送るように命じる。このインスタンスは、サイドFのインスタンスRLC(DC)へ通知を介して受信ACKを知らせ、サイドTのレイヤRRCにローカルメッセージAMD-REQ-CCCCを介して受信された通信を知らせる。サイドFでは、受信の通知ACKがインスタンスRLC(DC)によりレイヤRRCへローカルメッセージAMD-CON-CCCを介して送る。

【0073】サイドTでは、レイヤRRCは、インスタンスRLC(DC)へローカルメッセージAMD-REQ-CCOKを介して、通信AMD-PDU-CCOKをサイドFのインスタンスRLC(DC)へ送る。サイドFのインスタンスRLC(DC)はサイドTのイン

タンスRLC(DC)へ受信の通知ACKを介して通知し、そして、サイドFのレイヤRRCへ、受信された通信を介してローカルメッセージAMD-IND-CCOKを介して送る。サイドTでは、受信の通知ACKがインスタンスRLC(DC)によりレイヤRRCへローカルメッセージAMD-CON-CCOKを介して転送される。

【0074】今まで説明したメッセージと通信の交換は、手順CKC5のプロログとして参照される。通信AMD-PDU-CCCとAMD-PDU-CCOKは、古い暗号鍵で符号化される。これらの通信はRLCヘッダと呼ばれる制御情報を伴う制御部を有する。RLCヘッダの特別ビットC_kは、新たな暗号鍵又は古い暗号鍵のいずれかが使用されるのかを示す。この特別ビットC_kを使用するときには、手順CKC5に先立ち一度既に伝送され且つその受信がまだ通知されていないデータユニットは古い暗号鍵と共に再度転送されることができることが可能である。プロログ後に最初に送信されるときにはデータユニットは新たな暗号鍵で送信される。この手段は、繰返し伝送の場合には、聴者は、伝送の繰返しのフェーズ中にチャンネルを聞く場合には、常に既に受信された符号化されたデータユニットと同一のコピーを聞き且つ新たな情報を何も受信しない。

【0075】手順CKC5のプロログの前に、特別ビットC_kがゼロに設定される。特別ビットC_kが1に設定された後、次の同期フェーズで、データが新たな暗号鍵で符号化されることを示し、一方、同期フェーズで0に設定されたビットC_kは、データが古い暗号鍵で符号化されることを示す。

【0076】同期フェーズは端末と無線ネットワーク制御装置と異なる時間に開始し、；ダウンリンク(DL)では同期フェーズは、ローカルメッセージSTART-CKCS-DL及びSTART-CKCS-DT同期フェーズの開始のレイヤRLCのレイヤRRCがインスタンスRLC(DC)又はRLC(DT)に通知した後、第1のデータユニットDL-new-newの伝送と共に開始する。(ダウンリンクで送られた)データユニットは、プロログ後の最初に伝送されたとき、DL-new-newと呼ばれる。データユニットDL-new-newは、伝送の繰返しが起こるとすぐにデータユニットDL-newとなる。データユニットは(最初に又は繰返しとして)プロログ前に既に伝送されていれば、DL-old-oldと呼ばれる。データユニットは、プロログ後に再び伝送されるときには、DL-old-oldと呼ばれる。

【0077】アップリンク(UL)では、同期フェーズは最初のデータユニットUL-new-newの伝送で開始する。(アップリンクで送られた)データユニットは、最初のものでデータユニットDL-new-new又はDL-new後の最初に伝送されたとき、DL-new-n

ewと呼ばれる。データユニットDL-new-newは、再び伝送されるとすぐにデータユニットUL-newとなる。データユニットは、最初のデータユニットDL-new-new又はDL-newの繰返し前に既に伝送されていれば、UL-old-oldと呼ばれる。それは、最初のデータユニットDL-new-new又はDL-newの繰返し後にデータユニットDL-old-oldが繰返し伝送される場合には、データユニットUL-old-oldと呼ばれる。

【0078】以下の規則1から5は、同期フェーズを制御し、特別のビットC_kはゼロに設定され、アップリンクとダウンリンクの両方の後にそれぞれのデータユニットは新たな暗号鍵のみで符号化され、全データユニットUL-old-oldとDL-old-oldはいずれか成功的に(古い暗号鍵で符号化され)伝送され又は、伝送の許された繰返しの最大数はこれらのデータユニットに達する。最大数に達したときに、これらのデータユニットを伝送するのに更なる労力は成されない。

【0079】規則1：ダウンリンクの同期フェーズ中に、サイドFのレイヤRLC(例えば、インスタンスRLC(DC))は、新たな暗号鍵で符号化したデータユニットDL-new-new及びDL-newを送る。特別ビットC_kは1に設定されている。一方データユニットDL-old-oldは、特別ビットC_kが0に設定されている間は、古い暗号鍵で符号化し送られる。図14では、そのようなデータユニットはデータユニット番号26を有する。アップリンクの同期フェーズ中は、レイヤRLC(例えば、インスタンスRLC(DT))は、特別ビットC_kが1に設定されている間は、新たな暗号鍵で符号化したデータユニットDL-new-new及びDL-newを送る。データユニットDL-old-oldは、特別ビットC_kが0に設定されている間は、古い暗号鍵で符号化し送られる。

【0080】規則2：レイヤRLCは、エラーなしに受信された最初のデータユニットDL-new-new及びDL-newの連続のデータユニット番号SN(シーケンス番号)を蓄積する。このデータユニット番号は、RLCヘッダの一部を構成し、かつサイドTのSN_{F-old(T)}と呼ばれる。

【0081】図14では、SN_{F-old(T)}は、データユニット番号28を有する。シーケンス番号27を有する(図14)前に送られたデータユニットDL-new-newは、エラーなしに送られない。シーケンス番号27を有するデータユニットが再び送られるとき、このデータユニットはDL-newとなる。

【0082】サイドFのレイヤRLCは、最初に通知されたデータユニットDL-new-new及びDL-newの連続のデータユニット番号SNを蓄積する。このデータユニット番号は、SN_{F-old(F)}と呼ばれる。図14では、SN_{F-old(F)}は、データユニッ

19

20

30

40

50

ト番号28を有し且つデータユニットDL-new-newに属する。

【0083】規則3：サイドFのレイヤRLCは、エラーなしに受信された最初のデータユニットUL-new-new及びUL-newの連続の番号SN（シーケンス番号）を蓄積する。この番号は、 $SN_{F-UL}(F)$ と呼ばれる。図14では、それは、データユニット番号54を有し、データユニットUL-new-newより来る。一方データユニット番号53を有するデータユニットはデータユニットUL-oldである。一般的に以下が成り立つ。

$SN_{F-DL}(T) \leq SN_{F-DL}(F)$ 及び

$SN_{F-UL}(F) \leq SN_{F-UL}(T)$ 。

【0084】これらのデータユニット番号 $SN_{F-DL}(T)$ 、 $SN_{F-DL}(F)$ 、 $SN_{F-UL}(F)$ 、 $SN_{F-UL}(T)$ はプロローグフェーズ中は無効値が与えられる。データユニットのRLCヘッダから得たデータユニット番号は有効値である。

【0085】規則4： $SN_{F-UL}(F)$ が有効値を得たときのみ、ダウンリンク内の同期フェーズは終了されることができる。サイドFのレイヤRLCが全データユニットDL-oldとDL-newに関する通知を受信する。又は、全データユニットDL-oldとDL-newの伝送の繰返しの最大数に達すると終了される。サイドFのレイヤRLCはいつでもダウンリンク上で送信された全てのデータユニットを知っている。この判断ができる。ダウンリンクの同期フェーズの終了は、メッセージEND-CKCS-DL-Fを介してサイドFのレイヤRRCへ通知される。

【0086】ダウンリンク内の同期フェーズの終了は、サイドTで示され、特別ビット C_k がゼロに設定されたデータユニットDL-new-newが送られ、しかし新たな暗号鍵で符号化される。図14では、これと同様に送られる最初のデータユニットは、データユニット番号29を有する。サイドTのレイヤRLCは、特別ビット C_k がゼロに設定され受信されたデータユニットのデータユニット番号が、蓄積値 $SN_{F-DL}(T)$ より大きいとか又は等しいことからダウンリンク内の同期フェーズの終了を認識する。

【0087】ダウンリンク内の同期フェーズの終了後、サイドFのレイヤRLCは新たな暗号鍵と特別ビット C_k がゼロに設定されて符号化された全データユニットを送る。サイドTのレイヤRLCは、新たな暗号鍵で符号化されたデータユニットを受信する。

【0088】規則5：サイドTのレイヤRLCは、全データユニットDL-oldとDL-newが通知され又は、これらのデータユニットに対する伝送の繰返しの最大数に達することにより、アップリンク内の同期フェーズの終了を認識する。アップリンク内の同期フェーズの終了は、メッセージEND-CKCS-Tを介してサイ

ドFのレイヤRRCへ通知される。

【0089】アップリンクの同期フェーズの終了は、特別ビット C_k がゼロに設定されたデータユニットDL-new-newが送られ、しかし新たな暗号鍵で符号化され、サイドFに示される。図14では、これと同様の最初のデータユニットはデータユニット番号55である。サイドFのレイヤRLCは、特別ビット C_k がゼロに設定され受信されたデータユニットのデータユニット番号が、蓄積値 $SN_{F-UL}(F)$ より大きいとか又は等しいことからアップリンクの同期フェーズの終了を認識する。アップリンクの同期フェーズの終了は、メッセージEND-CKCS-Fを介してサイドFのレイヤRRCへ通知され、それにより新たな手順CKCSが再び開始される。

【0090】アップリンクの同期フェーズの終了後、サイドTのレイヤRLCは、新たな暗号鍵と特別ビット C_k がゼロに設定された符号化の形式で全データユニットを送る。そして、サイドFのレイヤRLCは、新たな暗号鍵で符号化されたデータユニットのみを受信する。

【0091】特別ビット C_k を使用することにより、手順CKCSは伝送のどのような中断も発生しないことが達成される。蓄積値 $SN_{F-DL}(T)$ 、 $SN_{F-DL}(F)$ 、 $SN_{F-UL}(F)$ 、 $SN_{F-UL}(T)$ を使用することなしに、手順CKCSをエラーなしで終了させることができない。

【0092】

【発明の効果】本発明により、異なる暗号変更手順を有する無線ネットワークを提供することできる。

【図面の簡単な説明】

【図1】無線ネットワーク制御装置と複数の端末を有する無線ネットワークを示す図である。

【図2】端末又は無線ネットワーク制御装置の種々の機能を説明するためのレイヤモデルを示す図である。

【図3】端末又は無線ネットワーク制御装置の符号化機能を説明するためのブロック図である。

【図4】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図5】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図6】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図7】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図8】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図9】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図10】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図11】符号化に必要な暗号鍵を変更する手順中の種

々の命令のルーチンを示す図である。

【図12】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図13】符号化に必要な暗号鍵を変更する手順中の種々の命令のルーチンを示す図である。

【図14】符号化に必要な暗号鍵を変更する手順中の種々

* 々の命令のルーチンを示す図である。

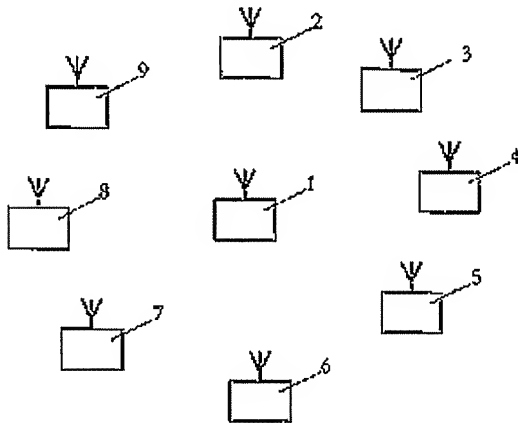
【符号の説明】

1 無線ネットワーク制御装置

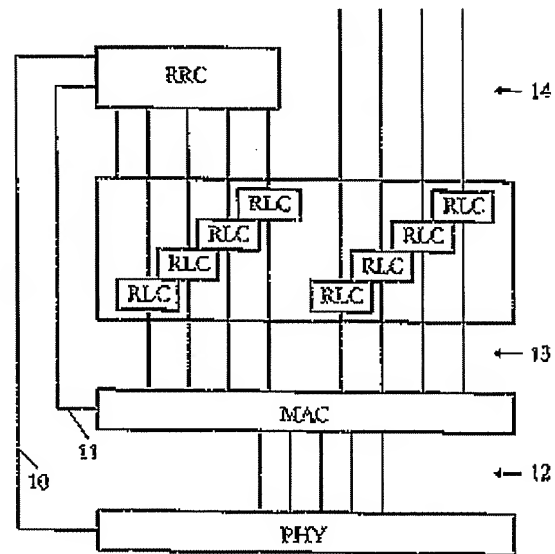
2から9 端末

16 符号化機能

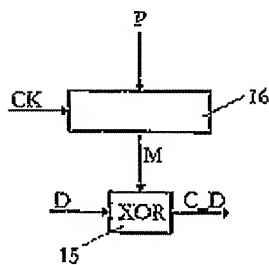
【図1】



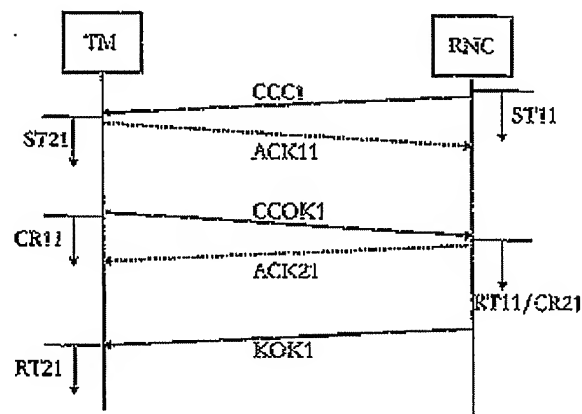
【図2】



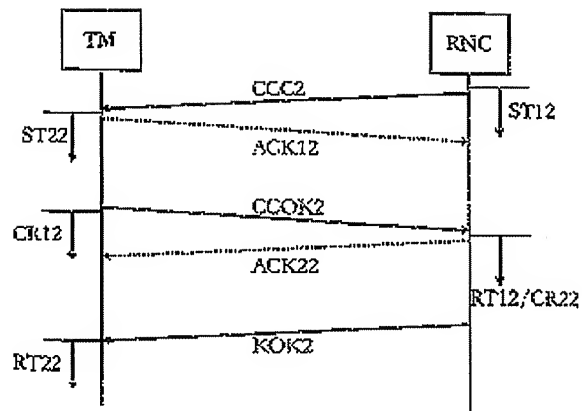
【図3】



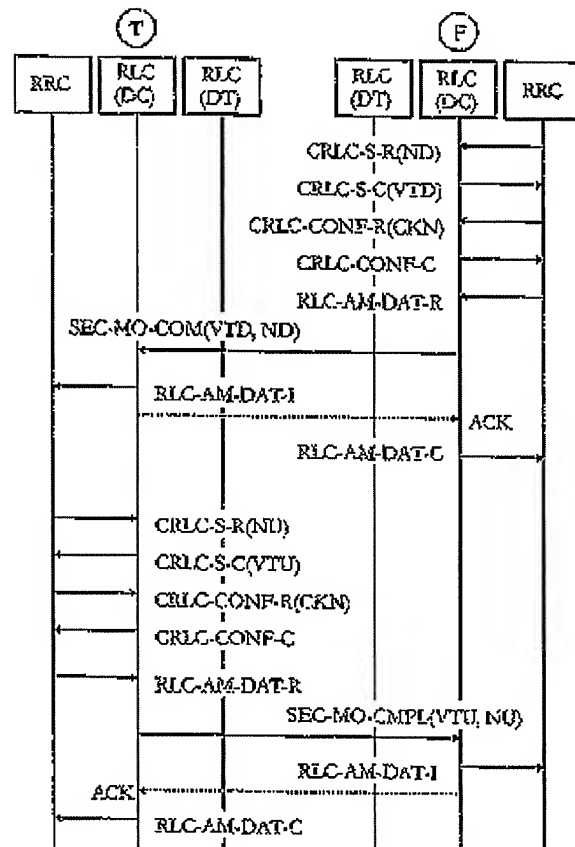
【図4】



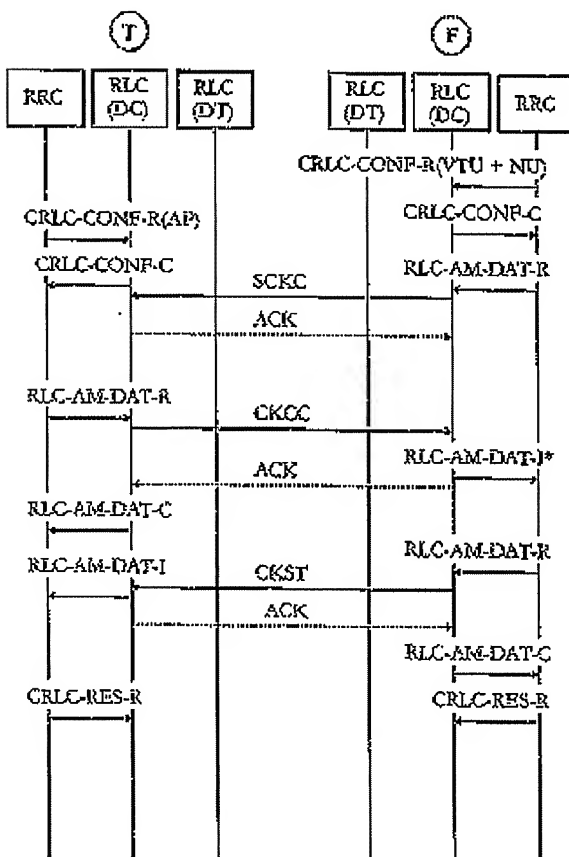
【図5】



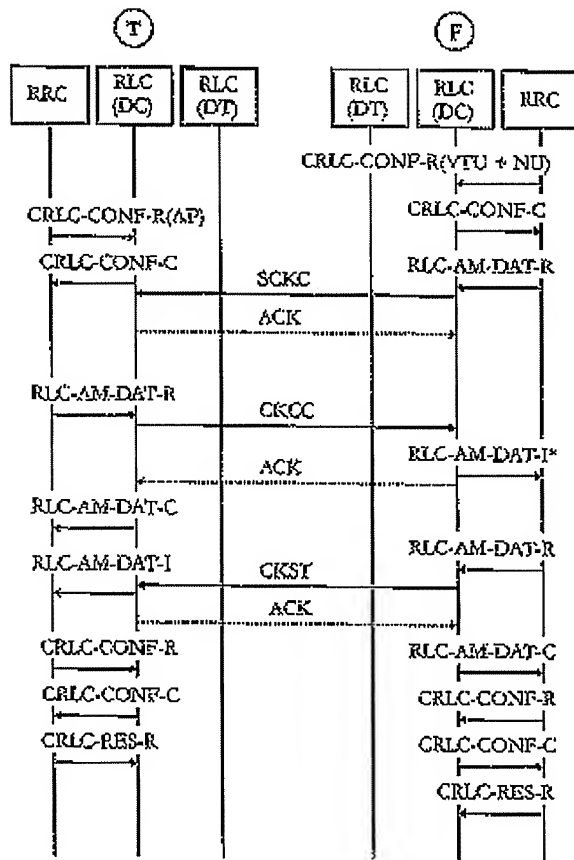
【図6】



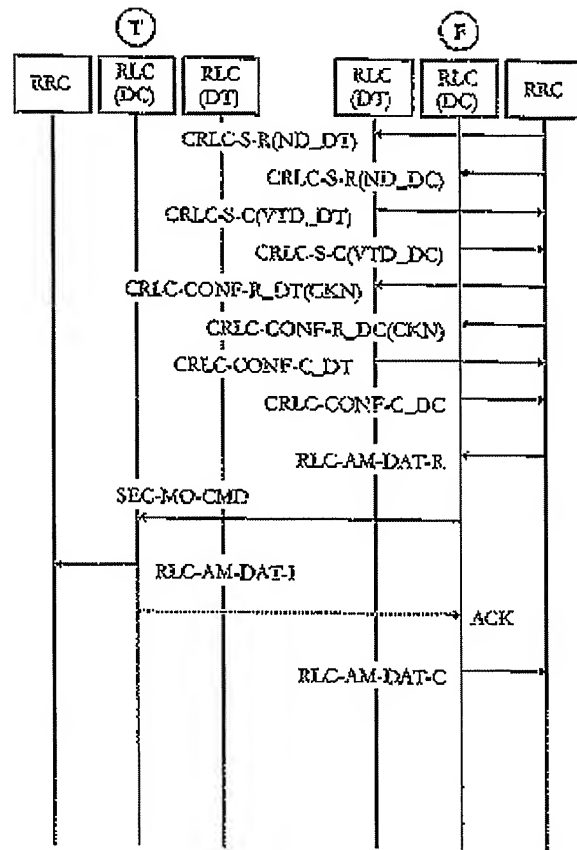
【図7】



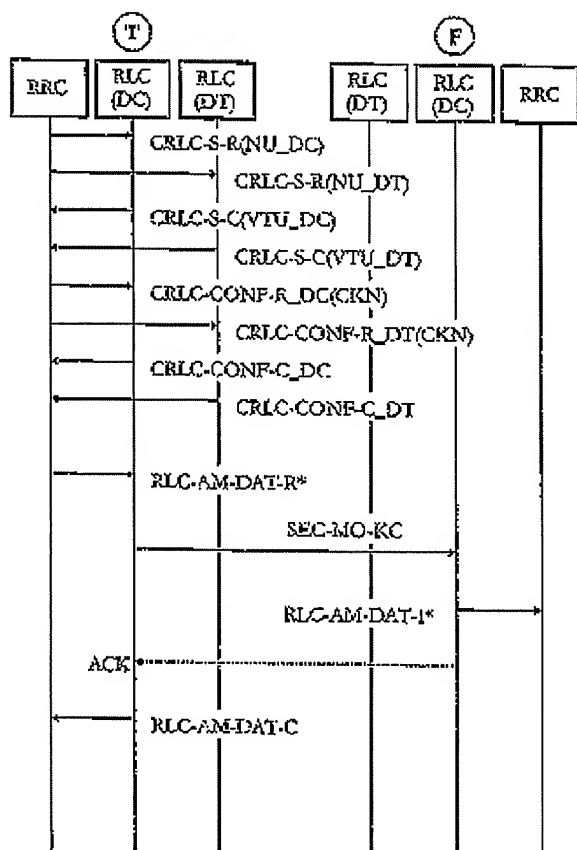
【図8】



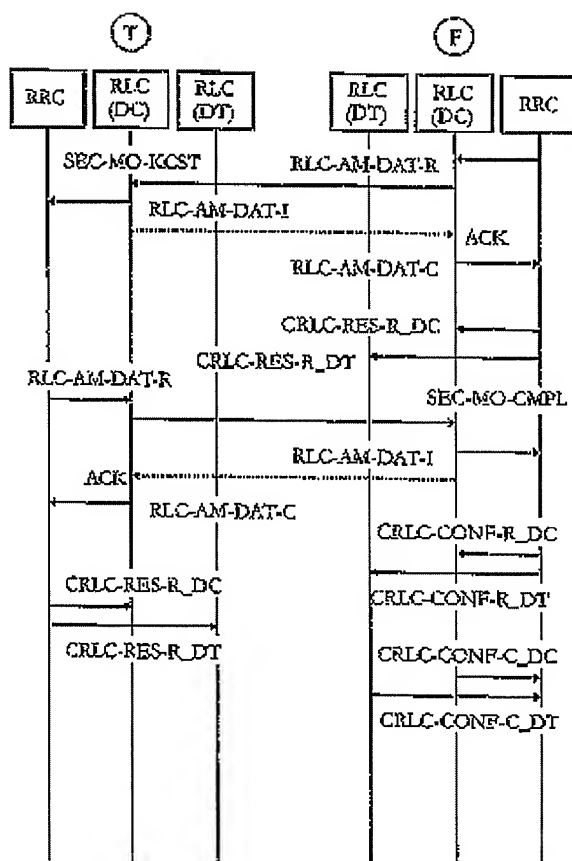
【図9】



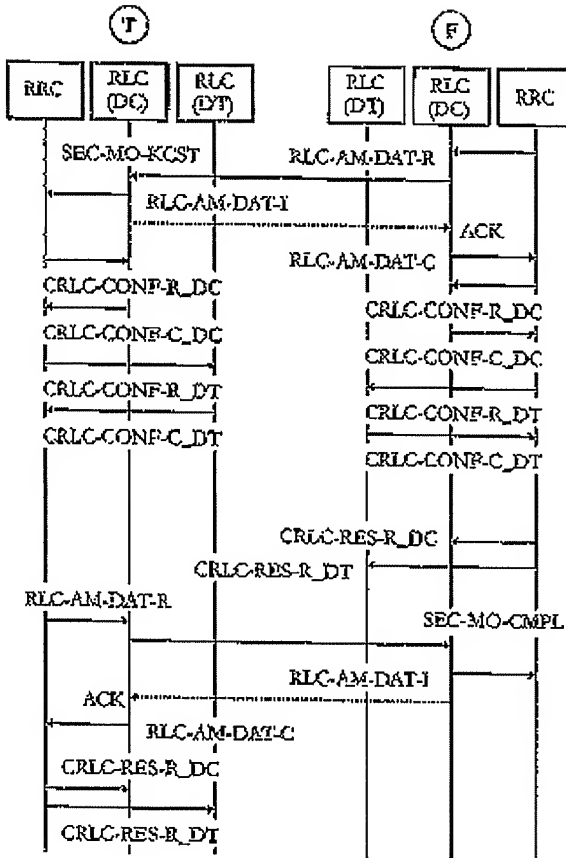
【図10】



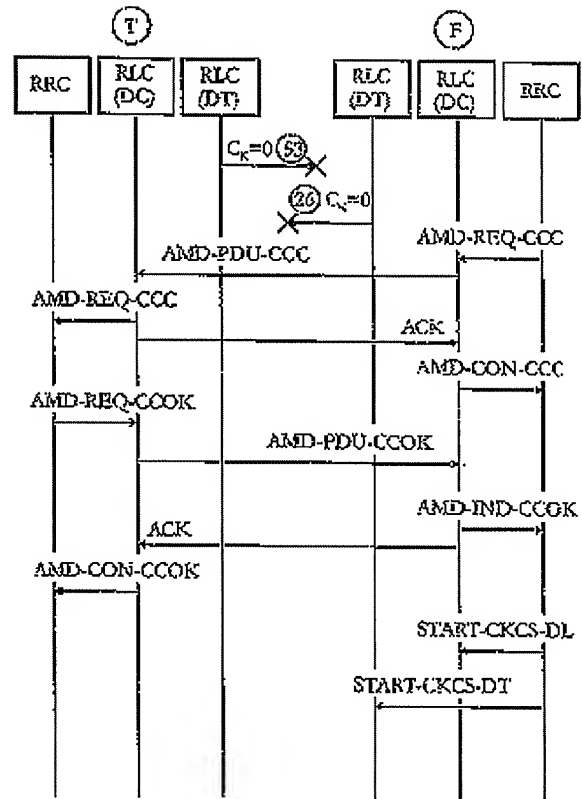
【図11】



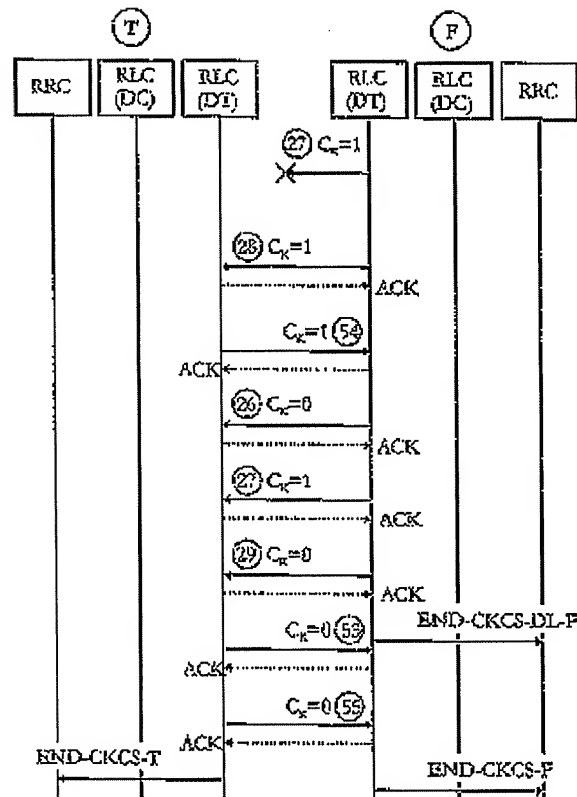
【図12】



【図13】



【図14】



フロントページの続き

(31)優先権主張番号 10002636.2
 (32)優先日 平成12年1月21日(2000. 1. 21)
 (33)優先権主張国 ドイツ(DE)
 (31)優先権主張番号 10015389.5
 (32)優先日 平成12年3月28日(2000. 3. 28)
 (33)優先権主張国 ドイツ(DE)

(71)出願人 590000248
 Groenewoudseweg 1,
 5621 BA Eindhoven, The
 Netherlands
 (72)発明者 ヨーゼフ ヴァッセル
 ドイツ連邦共和国, 50181 ベドブルク,
 シュタイフェンザントシュトラッセ 60